AO 91 (Rev. 02/09) Criminal Complaint

United States District Court
for the
Western District of New York

United States of America

v.

David Mondore

Defendant

Case No. 20-mj- 5176

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

(1) On or about December 3, 2019, in the Western District of New York and elsewhere, the defendant, DAVID MONDORE, intentionally accessed a computer without authorization and thereby obtained information from a protected computer and did so in furtherance of a criminal act in violation of the laws of New York State, that is, New York Penal Law § 155.25 and New York Penal Law § 190.78(1).

All in violation of 18 U.S.C. § 1030(a)(2)(C) and § 1030(c)(2)(B)(ii).

(2) On or about December 3, 2019, in the Western District of New York and elsewhere, the defendant, DAVID MONDORE, knowingly and with intent to defraud accessed a protected computer without authorization and by means of such conduct furthered the intended fraud and obtained something of value, that is, a photo of Victim 1.

All in violation of 18 U.S.C. § 1030(a)(4) and § 1030(c)(3)(A).

(3) On or about December 3, 2019, in the Western District of New York and elsewhere, the defendant, DAVID MONDORE, knowingly possessed and used, without lawful authority, a means of identification of another person, that is, a Snapchat account belonging to Acquaintance 1, during and in relation to a felony violation of Title 18, United States Code, Section 1030, committed in the manner set forth in the preceding two paragraphs, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

Complainant's signature

COREY P. LYONS
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION
Printed name and title

Sworn to before me and signed telephonically.

Date: July 31, 2020

Judge's signature

City and State: Buffalo, New York

HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, Corey Lyons, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since May 12, 2019. I am currently assigned to the Cyber Task Force, Buffalo Division. As part of the Cyber Task Force, I work on investigations relating to criminal and national security cyber intrusions. I received training on cyber matters during my time in Quantico, VA and have received private sector cyber training. I have worked or assisted with matters involving unauthorized access to computer systems, internet fraud, and business email compromises. My work in the FBI, as well as training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with criminal investigations. I have also conferred with other FBI Special Agents who have expertise and experience in cyber investigations and digital evidence.

2. I make this affidavit in support of an application for a criminal complaint and arrest warrant charging DAVID MONDORE with violating Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii) (unauthorized access to computer systems in furtherance of any criminal act in violation of state law); 1030(a)(4) and 1030(c)(3)(A) (unauthorized access to a protected computer in furtherance of fraud); and 1028A (aggravated identity theft). As described below, there is probable cause to believe that MONDORE obtained unauthorized access to victims' Snapchat accounts. After doing so, MONDORE saved digital copies of the victims' nude photos found in their Snapchat accounts; he changed the login information for each victim's Snapchat account, thereby prohibiting them from re-accessing their own account; and he assumed the identity of each victim on Snapchat in order to gain access to other Snapchat accounts belonging to his victim's friends and acquaintances.

3. As relevant here, Title 18, United States Code Section 1030(a)(2)(C) makes it a crime to "intentionally access[] a computer without authorization . . . and thereby obtain[] . . . information from any protected computer." Title 18, United States Code, Section 1030(c)(2)(B)(ii) makes a violation of Title 18, United States Code, Section 1030(a)(2)(C) a felony if a person violates Section 1030(a)(2)(C) "in furtherance of any criminal . . . act in violation of the . . . laws . . . of any State."

4. The predicate state law crimes underlying MONDORE's violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii) are (1) petit larceny, in violation of New York Penal Law Section 155.25; and (2) identity theft in the third degree, in violation of New York Penal Law Section 190.78.

a. New York Penal Law defines petit larceny as follows: "A person is guilty of petit larceny when he steals property." N.Y. Penal Law 155.25. The term "property" is defined to include "any . . . personal property [or] computer data." N.Y. Penal Law 155.00(1).

b. New York Penal Law defines identity theft in the third degree as follows: "A person is guilty of identity theft in the third degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby . . . obtains . . . property." N.Y. Penal Law 190.78(1).

5. Title 18, United States Code, Section 1030(a)(4) makes it a crime to "knowingly and with intent to defraud, access[] a protected computer without authorization . . . and by means of such conduct further[] the intended fraud and obtain[] anything of value."

6. Title 18, United States Code, Section 1028A makes it a crime to, "during and in relation to [a violation of, among other crimes, Title 18, United States Code, Section 1030], knowingly transfer[], possess[], or use[], without lawful authority, a means of identification of another person." 18 U.S.C. § 1028A(a). The term "means of identification" includes "any name or number that may be used, alone or in conjunction with any other information, to identity a specific individual." 18 U.S.C. § 1028(d)(7).

7. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, particularly agents from the Buffalo Field Office of the FBI, and private companies. Because this affidavit is submitted for the limited purpose of obtaining this criminal complaint and arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause.

PROBABLE CAUSE

A. Compromise of Victims' Snapchat Accounts

8. On or about December 5, 2019, the FBI received information regarding a potential compromise and victimization of a Snapchat account belonging to a State University of New York (SUNY) Geneseo student ("Victim 1").

9. Snapchat is a mobile application made by Snap Inc. and available through the iPhone App Store and Google Play. The application allows users to share photos, videos, and text with other users. Snapchat is primarily used for creating multimedia messages referred to as "snaps". Snaps can consist of a photo or a short video, and can be edited to include filters and effects, text captions, and drawings. Snaps can be directed privately to selected contacts or to a semi-public "Story". The private message photo snaps can be viewed for a user-specified length of time (1 to 10 seconds as determined by the sender). By holding down on the photo button while inside the app, a video of up to ten seconds in length can be captured. After a single viewing, the video disappears by default. A user takes a photo or video using his or her camera phone in real-time and then selects which of his or her friends to send

the message to. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender, and after the content is opened in the case of the recipient). Users are able to save a photo or video they have taken locally to their device or to "Memories," which is Snapchat's cloud storage service. Based on my training and experience, I know that Snapchat's servers are "protected computers" within the meaning of Title 18, United States Code, Section 1030, because they are "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

10. According to Victim 1, while at SUNY Geneseo, in Geneseo, New York, within the Western District of New York, she received a message from a Snapchat account owned by a person referred to herein as Acquaintance 1.

11. Victim 1 knew of Acquaintance 1 through a mutual acquaintance. The person messaging Victim 1 from Acquaintance 1's account asked Victim 1 for Victim 1's Snapchat login credentials under the ruse that Acquaintance 1 would use Victim 1's account to check whether "Acquaintance 1" had been "blocked" by another user.

12. Victim 1 provided her Snapchat login credentials to the person using Acquaintance 1's account and soon after received a text message from an UNSUB using the phone number +1(626)-515-8283. The text purported to be from Snapchat Security. The text message stated that Victim 1's Snapchat account had been locked and that she needed to provide a pin number to unlock it. The text message also advised that the pin requested would

be the same pin used for Victim 1's "My Eyes Only" folder in her Snapchat account. Victim 1 replied to the text message and provided the pin number for the folder. Shortly thereafter, Victim 1 received an email from the true Snapchat, notifying Victim 1 of a new device login to her account. The login was from an iPhone X using the internet protocol address 176.113.72.166 at 17:38:56 EST on December 3, 2019. The true Snapchat also notified Victim 1 that the email address associated with her account had been changed. After this occurred, Victim 1 was no longer able to access her account.

13. Victim 1 was later made aware that the person who had gained access to her Snapchat account had later used her account to send an explicit photo of Victim 1, which had been saved in her Snapchat account, to a large number of Snapchat users on her Snapchat friend list. (Records from Snapchat later confirmed that 116 of Victim 1's Snapchat contacts had received this photo from Victim 1's Snapchat account.) The photo was captioned, "Flash me back if we are besties." Four of Victim 1's friends responded back to the message, via Snapchat, by sending explicit pictures of themselves, one of whom was Acquaintance 2. Like Victim 1, Acquaintance 2 was a student at SUNY Geneseo at the time she responded to Victim 1's Snapchat account.

14. Acquaintance 2 stated that she received the message from Victim 1's account referred to in the previous paragraph. Once Acquaintance 2 replied with an explicit picture of herself, she noticed that Victim 1's Snapchat account saved the photo, which Acquaintance 2 noted was unusual for Victim 1 to do. On December 4, 2019, Acquaintance 2 received a text message from Victim 1 saying that her Snapchat account had been hacked and apologized if

anyone received suspicious messages from her. Acquaintance 2 then filed a police report fearing that the UNSUB who had accessed Victim 1's Snapchat account had the explicit photo Acquaintance 2 sent to Victim 1's account.

15. During an interview of Victim 1, she advised that multiple students from her hometown had their Snapchat accounts hacked in a similar way. Most, if not all, of the victims attended Bethlehem High School, located in Delmar, New York, and had some connection to Acquaintance 1.

B. Attribution of Snapchat Account Compromises to DAVID MONDORE

16. One of those victims, Victim 2, who lives in the Northern District of New York, filed a police report on December 7, 2019. According to Victim 2, his Snapchat account received messages from Acquaintance 3's Snapchat account requesting Victim 2's login credentials for his Snapchat account. The person operating Acquaintance 3's account claimed that she deleted her Snapchat account and wanted to login from Victim 2's account to confirm her account was deleted. Victim 2 then provided who he believed was Acquaintance 3 with his Snapchat login credentials. A short time later, Victim 2 received a text message from the phone number **+17278886881**. **+17278886881** claimed to be Snapchat Security and told Victim 2 that his account was locked due to suspicious activity. **+17278886881** then requested Victim 2's PIN number to unlock the account. **+17278886881** provided a hint for the PIN, saying it was the same as Victim 2's "My Eyes Only" folder PIN. After Victim 2 provided his login credentials and PIN, Victim 2 was locked out of his Snapchat account.

17. Subscriber information associated with Victim 2's Snapchat account revealed a login to the account from the IP address 172.241.166.77 on December 7, 2019 at 20:09:32 (EST). The subscriber information also shows a logout event from the same IP on December 7, 2019 at 21:59:22 (EST), indicating that the person was in Victim 2's Snapchat account during that two hour span. The chat transactional data from Victim 2's account shows that at 20:32:55 on December 7, 2019 (that is, after the account was accessed by the IP address 172.241.166.77) Victim 2's account sent a picture to 11 Snapchat users. This occurred while the UNSUB was in the account. The picture was a self-taken photo of erect male genitalia with the caption, "send a nude back." The UNSUB also engaged in chats with Snapchat users in an attempt to elicit nude photos from them.

18. Open source searches for the **+17278886881** phone number used to contact Victim 2 showed that the number was owned by Onvoy LLC. On or about December 23, 2019 a grand jury subpoena was served on Onvoy LLC for subscriber information associated with the **+17278886881** phone number. In response to the subpoena, Onvoy LLC indicated that the number had been sold to Twilio. On January 10, 2020, a grand jury subpoena was served on Twilio for subscriber information associated with the **+17278886881** phone number. In response to the subpoena, Twilio indicated that it had sold the number to another company called "Secret Phone".

19. Open source research into Secret Phone revealed that it is also known as Second Phone Number and is an application developed by a Florida based company called BP Mobile. The application is available through the Apple App Store and Google Play and allows users to acquire a private phone number for calls and texts. The application allows

users to pick a phone number and purchase credits that allow him or her to make calls and texts from that number. Users can choose a phone number from a list of available numbers in 25 different countries. Users are also able to view their text message history and forward calls to voice mail.

20. On January 23, 2020 a grand jury subpoena was served on BP Mobile for subscriber information associated with the **+17278886881** phone number. BP Mobile provided subscriber information, as well as IP login information and call log information. In addition, BP Mobile provided an additional phone number, **+17278886595**, that was used by the same customer. BP Mobile also voluntarily provided the content of text messages sent to and from **+17278886881** and **+17278886595**. Although BP Mobile voluntarily provided this information to the government, the government sought and received two search warrants to ensure that its review of the text messages complied with the Fourth Amendment.

21. Included in the subscriber information from BP Mobile were device models used by the UNSUB to access the BP Mobile application. The device models were listed as an iPhone X and an iPhone 11 Pro Max.

22. The text messages showed that on December 4, 2019, the **+17278886881** phone number (the number used to contact Victim 2) texted the word "Hello" to **+[redacted]0439**. Open source checks showed that the phone number **+[redacted]0439** belonged to a David MONDORE (MONDORE). The **+[redacted]0439** phone number received only the one message from **+17278886881** that said "Hello." This was the first message sent from the

+17278886881 number. Approximately two minutes earlier, **+[redacted]0439** had sent a text reading "Hi?" to **+17278886881**. The rest of the text messages on the **+17278886881** account involved the account owner messaging other phone numbers while pretending to be Snapchat security. By doing this, the UNSUB obtained passwords and security PIN numbers for over 20 Snapchat users. Examples of text messages sent by **+17278886881** and **+17278886595** to victims are as follows:

- Snapchat Security Alert – Your account has been temporarily locked due to unrecognized activity. To unlock the account, reply with your 4 digit PIN. Happy Snapping!
- For help with remembering your 4-digit PIN, reply with "HELP". Happy Snapping!
- Here's a hint – Your 4-digit account PIN by default would be the same as for your "My Eyes Only" section. Happy Snapping!
- Your password was recently changed. Reply with your newest password to successfully unlock the account. Happy Snapping!

23. I analyzed the IP login information that was associated with the **+17278886881** phone number and identified numerous Verizon Wireless IPs resolving to New York, New York. I also identified IP addresses owned by CyberGhost virtual private network (VPN) service[1] and a Clay, New York-based IP address (**74.111.33.161**), which was owned by Verizon FIOS, and which was accessed on December 24, 2019. A grand jury subpoena was then served on Verizon for subscriber information associated with the **74.111.33.161** IP address. In response, Verizon indicated that the owner of the subscription was [redacted] Mondore located at [redacted] CLAY, NY 13041. Open source searches

[1] A VPN extends a private network across a public network, enabling users to send and receive data across shared or public networks as if their devices were directly connected to the private network. Using a VPN allows users to mask their true IP address and access websites anonymously.

revealed that the [redacted] address was associated with a [redacted] Mondore (who was, at the time, 54 years old) and was previously associated with a David Mondore (who was, at the time, 28 years old). Based on the same associated address, last name, and difference in age, it is likely that [redacted] Mondore is the mother of David MONDORE.

24. Open source searches for David MONDORE revealed that he has a current address in New York, New York, where many of the IPs associated with the **+17278886881** phone number resolved. MONDORE's New York address is listed in a law enforcement database as [redacted] New York, New York 10027-7763. Open source searches also identified the email account [redacted]**@hotmail.com** as being associated with MONDORE. Open source searches for the [redacted]**@hotmail.com** account revealed that it was used as an Apple ID.[2]

25. On February 12, 2020, FBI Buffalo served a court order pursuant to 18 U.S.C. § 2703(d) to Apple for information associated with the [redacted]**@hotmail.com** Apple ID. The information FBI Buffalo received as a result of the § 2703(d) order showed that the [redacted]**@hotmail.com** Apple ID had an active iCloud account but that the Apple ID had not been used to purchase a BP Mobile application through Apple's App Store.[3] However, some of the IP logins to the iCloud account matched IP addresses used in the aforementioned

[2] Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

[3] iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups (for example, from an iPhone) and data associated with third-party apps.

+17278886881 Secret Phone account. Specifically, matching IPs from the CyberGhost VPN service, as well as an IP, **68.174.84.14**, associated with Spectrum residential service, were found on both accounts. Subscriber information from Spectrum indicated that the **68.174.84.14** IP address was registered to an individual with the following identifiers at the time of use:

Subscriber Name: [redacted]
Subscriber Address: [redacted] New York, New York 10027-7763
Username: [redacted]@gmail.com
Phone Number: [redacted]

26. Further, the § 2703(d) return showed that the iCloud account associated with [redacted]**@hotmail.com** was registered on two devices with the serial numbers DNQVQ7YAJCL8 and FK1ZJBMEN70H. The device models associated with these serial numbers were an iPhone X and an iPhone 11 Pro Max. Of note, and as mentioned in paragraph 21, these are the same device models used by the UNSUB to access the BP Mobile application Secret Phone, which was then used to trick Victim 2 into providing his Snapchat PIN. Finally, the Apple § 2703(d) returns indicated that [redacted]**@hotmail.com** had iCloud backup for iOS Devices (which would include an iPhone), iCloud drive, and iCloud Photos all enabled on the account.

27. On April 3, 2020, FBI Buffalo served another § 2703(d) court order to Apple for (1) any other Apple IDs associated with the device serial numbers described in paragraph 26; and (2) non-content information associated with those Apple IDs. The information FBI Buffalo received as a result of the § 2703(d) order showed that the [redacted]**@hotmail.com**

Apple ID was associated with the same devices as an additional Apple ID, [redacted]**@gmail.com**. The § 2703(d) returns also showed that the [redacted]**@gmail.com** Apple ID purchased multiple one-month subscriptions to BP Mobile's Second Phone Number service during and before the time period when victims' Snapchat accounts were compromised, as described above. As noted above, this was the same application used by MONDORE to text message victims while purporting to be Snapchat Security to elicit their login information from them. In addition, the returns showed that the user of the Apple ID [redacted]**@gmail.com** had purchased a BP Mobile subscription on December 3, 2019—that is, the same day that Victim 1's Snapchat account was compromised.[4]

28. The returns from Apple also showed that on October 27, 2019, the Apple ID [redacted]**@hotmail.com** was used to purchase 200GB of iCloud storage from Apple. Based on my training and experience, I know that 200GB of storage may be sufficient to save tens-of-thousands of images, as well as other data.

29. Review of the IP logins associated with the [redacted]**@gmail.com** Apple ID and the [redacted]**@hotmail.com** Apple ID showed IP usage similar to the IPs

[4] Comparing subpoena returns from BP Mobile and returns from the § 2703(d) order sent to Apple show a discrepancy (of up to one to two days) between the date when the user of [redacted]**@gmail.com** purchased a BP Mobile subscription through Apple and the date when, according to BP Mobile, a BP Mobile subscription was purchased. However, comparing these returns also shows logins to Apple and BP Mobile from the same IP addresses within a short timeframe. For example, the IP address 176.113.72.166 logged into the BP Mobile number **+17278886881** on December 3, 2019 at 18:57:49 PST. Returns from Apple show that that same IP address was used to purchase a one-month subscription to BP Mobile on December 3, 2019 at 18:57:56 PST—that is, seven seconds after the IP was used to log in to BP Mobile. That same IP address was also used to log into Victim 1's Snapchat account four times on December 3, 2019 between 14:38:55 and 18:00:30 PST.

used by the UNSUB to access Victim 1 and Victim 2's Snapchat accounts and the BP Mobile account. For example, on December 3, 2019, the IP address 176.113.72.166 was used to access the [redacted]**@gmail.com** Apple ID three separate times: 21:56:41, 21:57:56, 22:03:19. Of note, this is the same IP used by the UNSUB to log into Victim 1's Snapchat account on December 3, 2019 four times: 17:38:56, 19:06:06, 20:07:51, and 21:00:30. The 176.113.72.166 IP address was also used by the UNSUB to log into the **+17278886881** BP Mobile account (that is, the number used to contact Victim 2) on December 3, 2019 at 21:57:09. Based on this information, the 176.113.72.166 IP address was used on the [redacted]**@gmail.com** Apple ID, the **+17278886881** BP Mobile account, and Victim 1's Snapchat account within a one-hour timeframe. On December 8, 2019 at 20:47:05 EST, the [redacted]**@gmail.com** Apple ID used the IP address 172.241.166.77. Of note this is the same IP address referenced in paragraph 17 that was used by the UNSUB to access Victim 2's Snapchat account.

30. On April 30, 2020, FBI Buffalo served another § 2703(d) court order to Apple for iCloud services utilized by the Apple ID [redacted]**@gmail.com.** The information FBI Buffalo received as a result of the § 2703(d) order showed that the [redacted]**@gmail.com** Apple ID also utilized iCloud services. Specifically, the [redacted]**@gmail.com** Apple ID had enabled iCloud Drive and iCloud Photos. Both of these services can be used to upload and store photos from an Apple device, such as an iPhone.

31. On June 5, 2020, FBI Buffalo served a Search Warrant to Apple for content present on the iCloud accounts associated with the [redacted]**@gmail.com** Apple ID and the [redacted]**@hotmail.com** Apple ID. During review of the search warrant results, I identified a photo saved to the iCloud account associated to [redacted]**@hotmail.com**. This photo was of a separate phone screen. The separate phone screen shown in the picture displayed the previously referenced Snapchat conversation between Victim 1 and Acquaintance 1's Snapchat accounts. As Victim 1 had described, within the conversation, Victim 1 provided the person she believed to be Acquaintance 1 with her Snapchat login credentials. Further, the geo coordinates from the photo's metadata, [redacted], show that the photo was taken within approximately 62 feet of MONDORE's known address, [redacted]New York, NY 10027. Within the records associated to the [redacted]**@hotmail.com** iCloud account, I also located the known photograph of Victim 1 that was taken from her account and distributed to her Snapchat friends. This was the same photo I found in the Search Warrant returns from Victim 1's Snapchat account. In addition to Victim 1's photograph, I also located copies of each of the photographs that were sent by other victims to Victim 1's account, i.e., photos sent in response to the photo sent from Victim 1's Snapchat account reading "Flash me back if we are besties." I recognized these photos based on photos found in the search warrant returns from Victim 1's Snapchat account. I was able to further identify that these photographs were saved to the [redacted]**@hotmail.com** iCloud account. In addition to the Victim 1-associated photographs, I also located within MONDORE's iCloud account the explicit photographs sent to, and from, Victim 2's Snapchat account. These photos were originally discovered on the Search Warrant returns from Victim 2's Snapchat account. Again, these photographs were saved to the

[redacted]**@hotmail.com** iCloud account at the time that MONDORE had gained access to Victim 2's Snapchat account.

32. The Search Warrant to Apple also showed that both DNQVQ7YAJCL8 and FK1ZJBMEN70H devices (i.e., the two iPhones used to access the BP Mobile accounts described in this affidavit) were registered with the following information:

Name: David Mondore
Email Address: [redacted]@hotmail.com
Address: [redacted]New York, New York 10027-7762
Phone Number: [redacted]70439

The address associated with both of these iPhones is MONDORE's address. (The address above is interchangeable with [redacted] Further, the phone number associated with these iPhones is the same phone number used to send the first text message to the BP Mobile number **+17278886881**. As described above, the number **+17278886881** was used to trick Victim 2 into providing his Snapchat login credentials. In addition to the above, numerous photos of MONDORE were found on the [redacted]@hotmail iCloud account including photos of MONDORE's driver's license, Social Security card, and passport.

CONCLUSION

33. In sum, I respectfully submit that probable cause exists to believe that DAVID MONDORE committed violations of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii) (unauthorized access to computer systems in furtherance of any criminal act in violation of state law); 1030(a)(4) and 1030(c)(3)(A) (unauthorized access to a protected computer in furtherance of fraud); and 1028A (aggravated identity theft). I therefore request

that the Court issue the proposed criminal complaint and arrest warrant. I further request that the Court order the criminal complaint to be sealed until further order of the Court.

COREY LYONS
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me, telephonically, this
31st day of July, 2020.

HON. MICHAEL J. ROEMER
United States Magistrate Judge